UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/066,232	01/31/2002	Massimiliano Antonio Poletto	12221-010001	2754

26161 7590 01/29/2007

FISH & RICHARDSON PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
PERUNGAVOOR, VENKATANARAY	
ART UNIT	**PAPER NUMBER**
2132	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
2 MONTHS	01/29/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/066,232
Filing Date: January 31, 2002
Appellant(s): POLETTO ET AL.

Denis Maloney
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 11/6/2006 appealing from the Office action mailed 8/4/2006.

(1) Real Party in Interest

The real party of interest in the above application is Mazu Networks, Inc.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is incorrect. A correct statement of the status of the claims is as follows:

This appeal involves claims 1-36.

Claims 37-40 are allowed.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is substantially correct. The changes are as follows:

WITHDRAWN REJECTIONS

The following grounds of rejection are not presented for review on appeal because they have been withdrawn by the examiner. The Examiner rescinds the rejection for Claims 37-40 and after an updated search has found these claims allowable.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6769066	Botros et al.	7-2004
2002/0107960	Wetherall et al.	8-2002

(9) Grounds of Rejection

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States

only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 7, 9-14, 19-23, 26 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S Patent 6,769, 066 B1 to Botros et al.(hereinafter Botros).

Regarding Claim 7, 21, Botros discloses the producing of histogram of received network traffic based on parameters see Col 10 Ln 40-53 & Fig. 14 item 1402; characterization of attack based on comparison of historical histogram of data for parameter see Col 8 Ln 28-39 & Fig. 14 item 1404.

Regarding Claim 9 and 10, Botros discloses the varying of time to get an accurate historical data see Col 7 Ln 24-57.

Regarding Claim 11, 23, Botros discloses the normalizing of the histograms and computing the difference to significant outliner of suspicious traffic see Col 9 Ln 24-50.

Regarding Claim 13, Botros discloses the feature vector containing an list of anomalous behavior see Col 8 Ln 46-67.

Regarding Claim 12 and 14, 22, Botros discloses the correlation process that correlates the parameters and indicates the types of attacks see Col 13 Ln 24-41.

Regarding Claim 19 and 20, 26, Botros discloses the data collector see Fig. 3 item 202 and gateway see item 200.

Regarding Claim 21, Botros discloses the computing device see Fig. 2 item 104, producing of histogram of received network traffic based on parameters see Col 10 Ln 40-53 & Fig. 14 item 1402; characterization of attack based on comparison of historical histogram of data for parameter see Col 8 Ln 28-39 & Fig. 14 item 1404.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-6, 8, 15-18, 24-25, 27, 30-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S Patent 6,769, 066 B1 to Botros et al.(hereinafter Botros) in view of U.S. Patent 2002/0107960 A1 to Wetherall et al.(hereinafter Wetherhall).

Regarding Claim 1, 28, Botros discloses the monitoring of device for attacks where detecting process to determine if the parameter of network traffic exceed normal value see Col 10 Ln 40-53 & Col 9 Ln 1-23; a process to build histogram for the parameter to

compute significant outliers in a parameter and classify the attack see Fig. 9 item 904 & Fig. 10. But does not disclose a filtering of network packets based on the characterization process. However, Wetherall discloses the filtering processes based on the characterization process using histogram for parameter to compute significant outliers in a parameter and classify the attack see Fig. 2 item 206, 208, 210, 212.It would be obvious to one having ordinary skill in the art at the time of the invention to include the filtering processes based on the characterization process using histogram in the invention of Botros in order to route out the undesirable packets as taught in Wetherall see Par. 0041.

Regarding Claim 2, Botros discloses the vector having bad and good values see Col 9 Ln 51-Col 10 Ln 3.

Regarding Claim 3, Botros discloses the correlation process that correlates the parameters and indicates the types of attacks see Col 13 Ln 24-41.

Regarding Claim 4, Botros discloses the correlation process being used for reduce false positives see Col 12 Ln 59-Col 13 Ln 3.

Regarding Claim 5 and 6, 29, Botros does not discloses the aggregate filtering. However, Wetherall discloses the aggregate filtering see Par. 0041(blanket filtering) and

source IP address see Fig. 2 item 208 & 212. For motivation to combine see above Claim 1.

Regarding Claim 8, 30-31, Botros discloses the comparison of historical data for ranges see Col 10 Ln 40-53, but does not disclose the filtering process. However, Wetherall discloses the filtering processes based on the characterization process using histogram see Fig. 2 item 206, 208, 210, 212.It would be obvious to one having ordinary skill in the art at the time of the invention to include the filtering processes based on the characterization process using histogram in the invention of Botros in order to route out the undesirable packets as taught in Wetherall see Par. 0041.

Regarding Claim 15-18, 24, 27, Botros does not discloses the producing of a vector that is constant and constructing a vector for packets to test whether to forward for drop packets from source address. However, Wetherall discloses the producing of a vector that is constant and constructing a vector for packets to test whether to forward for drop see Par. 0056. It would be obvious to one having ordinary skill in the art at the time of the invention to include the filtering processes based on the characterization process using histogram in the invention of Botros in order to route out the undesirable packets as taught in Wetherall see Par. 0041.

Regarding Claim 25, Botros does not disclose the dynamically installing of filters on nearby routers. However, Wetherall discloses the installing of filters on routers see Fig. 1 item 106d & Fig. 2 item 210.

Regarding Claim 32, Botros discloses the monitoring of device for attacks where detecting process to determine if the parameter of network traffic exceed normal value see Col 10 Ln 40-53 & Col 9 Ln 1-23 through a gateway see Fig. 2 item 104; a process to build histogram for the parameter see Fig. 9 item 904 & Fig. 10 and comparing it with a historical histogram for a parameter see Col 8 Ln 28-39 & Fig. 14 item 1404. But does not disclose a filtering of network packets based on the characterization process using histogram. Botros further discloses the comparison of historical data for ranges see Col 10 Ln 40-53, but does not disclose the filtering process. However, Wetherall discloses the filtering processes based on the characterization process using histogram see Fig. 2 item 206, 208, 210, 212.It would be obvious to one having ordinary skill in the art at the time of the invention to include the filtering processes based on the characterization process using histogram in the invention of Botros in order to route out the undesirable packets as taught in Wetherall see Par. 0041.

Regarding Claim 33-36, Botros discloses the communicating of statisitics to data center over an secure networks see Fig. 3.

(10) Response to Argument

1. Claims 7, 9-14, 19-23, 26 are unpatentable over Botros.

Claims 7, 19, 20, 21 and 26

The Appellant's arguments regarding claim 7 and 21 are not persuasive. As Botros discloses the producing of an histogram of received network traffic see Col 3 Ln 37-51 & Fig. 10 & Fig. 11. The network traffic disclosed by Botros includes the user activities and peer activities collectively being stored on a data store for comparison to detect abnormal behavior thorough the use of a histogram see Col 4 Ln 17-25. Where the network is being examined initially to collect data on the users on the network and form a distribution of users, i.e. histogram see Col 3 Ln 37-44. Botros discloses the raw data collected include the data of commands performed, user activities see Col 6 Ln 53-62. Botros further goes on to mention a features list containing information about the violations, user activities, computer and network loads were this list used in generation of an histogram to be used for detection of abnormal behavior see Col 5 Ln 67- Col 6 Ln 4. And additionally, Botros mentions the user activity being divided into more categories to collect data for building a histogram including monitoring of file access, resource usage, login failures, whereby the listing suggests network traffic see Col 7 Ln 11-23. In that, resource and files are most likely shared on a network through a server and monitoring of these characteristics suggests a monitoring of network traffic. And the network traffic is being used to build a histogram and an second histogram for anomalous behavior see Col. 10 Ln 40-65.

The Appellant's argument regarding the characterizing an attack based on comparison of an historical histogram and produced histogram is not persuasive. Botros discloses such an histogram, where historical data is collected to form an histogram and later compared with a current histogram to detect anomalous behavior, i.e. attack, see Col 10 Ln 18-65. Where the intrusion is detected by the anomalous behavior by comparing of the histogram collected during normal activity and deviation from that histogram is suggestive of an anomalous activity, i.e. attack see Col 10 Ln 18-65. Botros goes on to mention the collecting of data during a time period sufficient to proper define normal behavior, thus being able to gauge intrusion see Col 10 Ln 29-39. And this histogram is normalized between –5 to 5 to clearly point out anomalous behavior see Col 10 Ln 40-53. As such, the system knows what to expect on the network and when deviations occur it can clearly pick it out. Botros goes at length about historical data files and user activity files being used to extract features see Fig. 2 item 12, 102, 104. This feature is being used to generate a histogram, i.e. model, to generate an score to indicate intrusion see Fig. 2 item 108,110. Botros is replete with references to comparing of historical histogram to a current histogram to detect intrusion see Fig. 4 item 304, 306, 308. Where the references to standard deviation, mean, sum are all in parlance of generating of histograms.

Botros' intrusion detection system is used primarily to detect the abnormal behavior of the users and network traffic. Although, Botros discloses a neural network model, such a model functions to do exact what the instant invention claims, namely to characterize

attacks see Col 10 Ln 66- Col 11 Ln 12. And this model goes further by sampling thousands of network traffic to accurately reflect the abnormal behavior see Col 11 Ln 5-11.

Claim 9 and 10

The Appellant's arguments regarding the time periods is not persuasive. As Botros discloses the time periods being varied from 4 to 6 months see Col 10 Ln 29-39. And further, the time being varied accordingly to get a desired degree of accuracy, and further suggests gathering thousands of values over an range X in a given time period T see Col 10 Ln 29-39 & Col 7 Ln 1-5. Botros additionally talks about a predetermined period of collecting data see Col 10 Ln 29-39.

Claims 11-14

The Appellant's arguments regarding the difference is not persuasive. Botros discloses the computation of the difference in the historical and produced histograms see Col 9 Ln 39-44. And Botros discloses specifically the difference being calculated to detect anomalous behavior see Col 11 Ln 57-61. Botros discloses the normalizing of data used in the histogram to –5 to 5 and further calculating the deviation, i.e. difference, from normal behavior see Fig. 6 item 604, 606.

Claim 19, 20, and 26

The Appellant's arguments regarding the absence of a data collector and executing of a function is not persuasive. As Botros discloses just such a function, where database is

database is maintained regarding user activity see Fig. 2 item 12 & Fig. 3 item 204, and feature generator for extracting information from the database see Fig. 2 item 104. Botros further discloses the user activity database interfacing with the expert-system in intrusion detection see Fig. 1 item 12.

Claims 22 and 23

The Appellant's arguments regarding correlating parameters to reduce legitimate traffic is not persuasive. As Botros discloses the setting of probabilistic parameters accurately to reduce "false positive" and not to be desensitive to intrusions see Col 12 Ln 52- Col 13 Ln 3. Where the factor is being adjusted to capture the intrusions and to avoid false alerts, thereby reducing blocking legitimate traffic.

2. Claims 1-6, 8, 15-18, 24-25, 27, 30-36 are unpatentable over Botros in view of Wetherall.

Claims 1, 3 and 4

The Appellant's arguments regarding the values exceeding normal values for the parameters to indicate attack are not persuasive. Appellant's arguments regarding the parameter of network traffic is argued above. Turning to the arguments regarding exceeding of normal values is disclosed by Botros in the same terms as the instant invention see Col 9 Ln 31-46. Where the abnormal behavior is detected by the ratio, and histogram being skewed to a certain end either –5 or 5 see Col 47-53. And

additionally, the Examiner asserts that standard deviation of Botros can reveal the abnormality of a certain histogram. As a large deviation would be suggestive of more or less frequency of action thus indicative of an intrusion as Botros discloses. And Botros makes the link between historical standard deviation and current standard deviation see Fig. 6 item 604, 606. The parameters are also being used to generate a histogram and to be compared with historical histogram, the deviation in form of a score is used to indicate attack see Col 9 Ln 51- Col 10 Ln 16. Reflecting the changes in deviation is done through normalizing the data and looking for a skew in graph like in Fig. 11 and its deviation from a bell curve like that of Fig. 10. Further, Botros discloses a use of an set desired score to look for deviation from the set desired score to indicate abnormal activity see Fig. 14 item 1410. Effectively, Botros discloses the exceeding of normal values to indicate attack in many forms-ratio, skew in histogram, standard deviation of scores, and set desired score.

The Appellant's second argument regarding the parameters to compute significant outliers and classifying of attack is not persuasive. At the outset, the Appellant has misunderstood the rejection. The error on part of the Examiner was to say that Botros does not disclose the parameters to compute significant outliers and classify attacks. That is clearly indicated by Botros as argued above, with regard to parameters exceeding normal values relating to significant outliers and thus classifying attack. It is believed the Appellant had some idea of the misstatement, as the Brief goes on to

mention the filtering process based on characterization process being the main argument.

Accordingly, Wetherall does disclose the filtering packets based on characterization process see Par. 0010 & Fig. 2 item 208. Where the packets originating from an spoof or bad address is filtered out. And the spoof address is determined by a histograms of the source address and determining if it diverges from the expected behavior see Par. 0028 & Fig. 13b. Additionally, the address is designated as a spoof address if it exhibits behavior based on timing and frequency of behavior see Fig. 13c, axiomatic of Bortos's invention. Wetherall construct a profile, i.e. histogram, for the source address based on number of characteristics, including migration, destination consistency and source address range see Par. 0012. One objective of Wetherall includes thwarting of Denial of Service attacks(DoS), which is the main objective of the instant invention see Par. 0006. Finally, Wetherall discloses the comparing of historical profile, i.e. histogram with an generated histogram to indicate an attack and further of filtering of the packets from corrupted source see Par. 0039. Thus, Wetherall discloses the instant invention to the extent disclosed in the claims, where the historical histogram is compared with a current histogram to classify attack and further of filtering the address based on the histograms.

The Appellant's argument regarding the modifying of Botros with Wetherall would not serve any purpose of Botros is not persuasive. As Botros deals with generation of histograms and comparing of historical histograms for attack. Similarly, Wetherall deals

with generation of histograms and comparing of historical histograms to classify attacks, further advancing Botros by the inclusion of filters serving to eliminate spoofed addresses. Thus, both pieces of prior art are relevant to the instant invention and both disclose to an great detail the instant invention.

Claim 2 and 5

The Appellant's arguments regarding bit vectors is not persuasive. As Botros discloses the ratio containing a mixture of bad and good values see Col 12 Ln 37-39. And further discloses the summing of values and containing number of instances to calculate standard deviation see Fig. 4 item 308. Further, the vector is axiomatic of the sum_i notation, whereby the sum values are calculated for i-th term of an n length vector. The bits are represented within the vector to include good and bad values in way of calculation leading to the standard deviation illustrating attacks. Finally, Wethrall's profile(bit vector), broadly speaking since it is embodied within an computer consists of bits, is being used as a reference for future comparison to detect attacks.

Claim 6

The Appellant's argument regarding the parameters being used to classify attack is not persuasive. As Wetherall discloses the source address being used to gather data for generation of a histogram and further of the histogram being used to compare the historical histogram further filtering of packets see Par. 0012. The parameters including

source address range, frequency and volume see Fig.14a-14d. The parameters may include timings, migration and other factors see Par. 0012.

Claim 8

The Appellant's argues nothing new in this section, but the absence of a bit vector. For a rebuttal, please see Examiner's argument in Claim 2 and 5.

Claim 15-17

The Appellant's arguments regarding the master correlation vector is not persuasive. As Wetherall discloses the reference profile being used to compare with current profile see Par. 0056. And this is done through the use of digitalizing the data, i.e. bit vector, and further comparing thorough viewing resemblance to the reference profile, bit vector, see Par. 0036-0037. And further, the reference profile is constant-time, independent of other profiles see Par. 0040.

Claim 18

See arguments for Claim 6 above.

Claim 25

The Appellant argues the motivation to combine, which is already discussed Claim 1, 3 and 4 above.

Claim 32, 35 and 36

The Appellant's only argument appears to be that filtering using histogram to characterize attacks is not being disclosed by Wetherall. However, Examiner respectfully disagrees. Wetherall discloses just such a function, where filtering occurs as a response to abnormality to expected condition illustrated through a histogram see Par. 0056-0057. In that, similar to Botros an historical/reference histogram is being compared with a generated histogram to indicate an spoof address see Fig. 10. And further, when a spoof address has been indicated additional processing occurs to filter out spoof sources, i.e. source of corrupt data/attack see Fig. 11. Wetherall is replete with disclosure of histograms being generated on different characteristics(e.g. source, destination, timing, frequency) being used to alert of an attack and further of filtering out of these instances see Fig.2 & Fig. 14a-14d. As such, these profile, i.e. histograms are further precautioned to make sure non-spoof addresses are not filtered out see Par. 0040-0041. These extra measures are being taken in form of analyzer, notifier and alert regulator see Par. 0056. Thus Wetherall discloses the filtering based on characterization process using histograms.

The motivation is combine is also argued here as in Claim 1, 3 and 4 above. And the Examiner asserts the same reasoning as above.

Claim 33 and 34

The Appellant's arguments with regard collecting of statistics from gateway are not persuasive. As Botros discloses the very same in form a log and a database see Fig. 2

item 12 & 102. And this feature is also illustrated in Fig. 1 as user activity database see item 12.

Lastly, the dedicated network for communications is also being disclosed by Botros see Fig. 1 & Fig. 2, where the direction of flow is unidirectional thus indicative of a dedicated network. And additionally, Botros discloses buses to interface with networks and storage see Fig.15.

Claim 37

The Appellant's arguments are persuasive. And after an updated search, the Examiner has found the subject matter allowable.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Venkat Perungavoor

Art Unit 2132

Conferees:

KAMBIZ ZAND
PRIMARY EXAMINER
SPE 2134

Kim Vu

KAMBIZ ZAND
PRIMARY EXAMINER

Kambiz Zand